GAU 2766
2131
#4

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Alexandre F. Tenca, Çetin K. Koç

Art Unit: 2766

Application No. 09/621,020

Filed: July 21, 2000

For: SCALABLE METHODS AND APPARATUS FOR MONTGOMERY MULTIPLICATION

Examiner: --

Date: December 4, 2000

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on December 4, 2000 as First Class Mail in an envelope addressed to: COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231.

Michael D. Jones
Attorney for Applicant

INFORMATION DISCLOSURE STATEMENT PURSUANT TO 37 C.F.R. § 1.97(b)(3)

TO THE COMMISSIONER FOR PATENTS
Washington, DC 20231

Sir:

Listed on the accompanying form PTO-1449 and enclosed herewith are several English-language documents. Applicants respectfully request that these documents be listed as references cited on the issued patent.

Applicants filed this Information Disclosure Statement before the mailing date of a first Office action on the merits. However, if the Patent Office determines that a fee is required for Applicants to file this Information Disclosure Statement, please charge any such fees, or credit overpayment, to Deposit Account No. 02-4550. A **duplicate** copy of this Information Disclosure Statement is enclosed.

Respectfully submitted,

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP

By
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

#4

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53434	Ser. No.: 09/624,000
	Applicant: Tenca et al.	
	Filed: July 21, 2000	Art Unit: 2766

OTHER DOCUMENTS

			Kaliski, Jr., B.S., "The Montgomery Inverse and Its Applications," IEEE Trans. on Computers 44:1064-1065 (August 1995)
			Montgomery, P.L., "Modular Multiplication Without Trial Division," Math. of Computation 44:519-521 (April 1985)
			Koç, Ç.K. et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," IEEE Micro 16:26-33 (June 1996)
			Dhem, J. et al., "SCALPS: Smart Card For Limited Payment Systems," IEEE Micro 16:42-51 (June 1996)
			Diffie, W., Hellman, M.E., "New Directions in Cryptography," IEEE Trans. on Information Theory 22:644-654 (1976)
			Rivest, R.L. et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21:120-126 (1978)
			Koç, Ç.K., Acar, T., "Fast Software Exponentiation in GF(2^k)" in Proceedings, 13th Symposium on Computer Arithmetic, pp. 225-231 (July 1997) (T. Lang et al., editors)
			Hamano, T. et al., "$O(n)$-Depth Circuit Algorithm for Modular Exponentiation" in Proceedings, 12th Symposium on Computer Arithmetic, pp. 188-192 (July 1995) (S. Knowles, W.H. McAllister, editors)
			Orup, H., "Simplifying Quotient Determination in High-radix Modular Multiplication" in Proceedings, 12th Symposium on Computer Arithmetic, pp. 193-199 (July 1995) S. Knowles, W.H. McAllister, editors)

EXAMINER:	DATE

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.

#4

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53434	App. No. 09/621,020
	Applicant: Tenca et al.	
	Filed: July 21, 2000	Art Unit: 2766

OTHER DOCUMENTS

			Bernal, A., Guyot, A., "Design of a Modular Multiplier Based on Montgomery's Algorithm" in 13th Conference on Design of Circuits and Integrated Systems, pp. 680-685 (November 1998)
			Eldridge, S.E., Walter, C.D., "Hardware Implementation of Montgomery's Modular Multiplication Algorithm," IEEE Trans. Computers 42:693-699 (June 1993)
			Kornerup, P., "High-Radix Modular Multiplication for Cryptosystems" in Proceedings, 11th Symposium on Computer Arithmetic, pp. 277-283 (June 1993) (E. Swartzlander et al., editors)
			Walter, C.D., "Space/Time Trade-offs for Higher Radix Modular Multiplication Using Repeated Addition," IEEE Trans. Computers 46:139-141 (1997)
			Royo, A., et al., "Design and Implementation of a Coprocessor for Cryptography Applications," European Design and Test Conference, pp. 213-217 (March 1997)
			Koç, Ç.K., Acar, T., "Montgomery Multiplication in GF(2k), "Designs, Codes and Cryptography 14:57-69 (1998)
			Tenca, A.F., "Variable Long-Precision Arithmetic (VLPA) for Reconfigurable Coprocessor Architectures," Ph.D. Thesis, University of California at Los Angeles (March 1998)

EXAMINER:	DATE

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.